Mõttekad kulutused infoturbele

VÕITLUSE VÄLTIMATUSE PRINTSIIP:
Süsteemide maailmas on võitlus (sh ressursside hankimise ja omamisega seotud võitlus) vältimatu.
Peeter Lorents “Süsteemse käsitluse alused”

Jüri Kivimaa
jyri.kivimaa@mil.ee

Üldjuhul ei tulda infoturbeks ressursse pakkuma –
need tuleb IT'l/infoturbel ise põhjendada ja välja võidelda.

Kust ja kuidas saada vajalikud ja usaldatavad numbrid ?

Abiks on üldtunnustatud metoodikad ja neil
põhinevad standardid (?).

Päris nii lihtne see ikka pole – ka olemasolevate standardite korral (ja andmeturbest on neid üksjagu) on küllaltki tihti olulisi ja tegelikult vastuseta (vähemalt piisavalt täpse vastuseta) jäävaid küsimusi.

Teoreetiliselt on asi imelihtne – lahendada tuleb rentaablusülesanne, kus võrreldakse prognoositud kahju (riske) turvameetmetele tehtavate kulutustega ja need kulutused peavad olema kasulikud.

Aga kuidas määratleda seni toimumata ja suurte potentsiaalsete kahjudega ohtude tõenäosust ?

Kui rakendame mingi konkreetse ohu vastu mingi konkreetse turvameetme – kas me tõesti julgeme väita, et teame küllalt täpselt uut riski ?
Loodame, et oht välistatud ?

Kui efektiivsed meie konkreetsed infoturbe lahendused tegelikult on ?

Päris lõplikke vastuseid/lahendusi (veel) pole, kuid teadmine, et miski on raske või ei teki täit lahendust, ei tähenda, et asjaga üldse tegelema ei peaks.

Jagan eelneva küsimuse kaheks:

1. Kui palju on majanduslikult otstabekas/mõttekas kokku infoturbeks ressursse (põhiliselt raha ja inimesi – st sisuliselt ikkagi raha) kulutada ? Teiste sõnadega – kuidas määratleda kaitstava info väärtus ? Sest oleks ju rumal kulutada turbeks rohkem kui info väärt on.

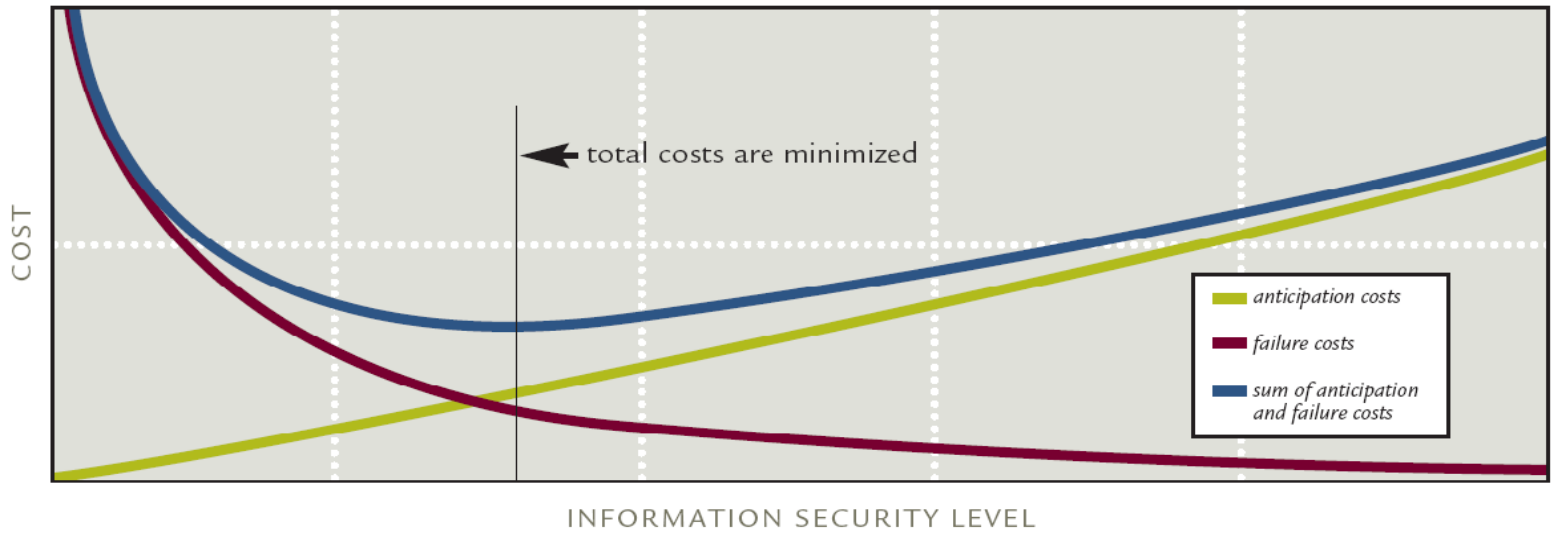
2. Kuidas jagada see otstarbekas/mõttekas kogukulutus otstarbekalt infoturbe tegevusvaldkondade vahel ?
   Pidades silmas, et raha on üldjuhul vähem kui vaja ja et keti tugevuse määrab tema nõrgim lüli.

Kui palju on mõistlik infoturbeks kulutada ?

1. metoodika

Infoturbega seotud kulud kokku = turvaintsidentide vältimiseks tehtud kulutused (ennetavad turvameetmed) + toimunud turvaintsidentidest tingitud kahjud (saamata jäänud tulud + sanktsioonid + taastamiskulud).

Üldprintsiip – **tuleb leida turvaintsidentidest tingitud kahjude ja infoturbe kulutuste summa miinimum.**



Turvatase = Tõrjutud ründed / Kõik ründed ???

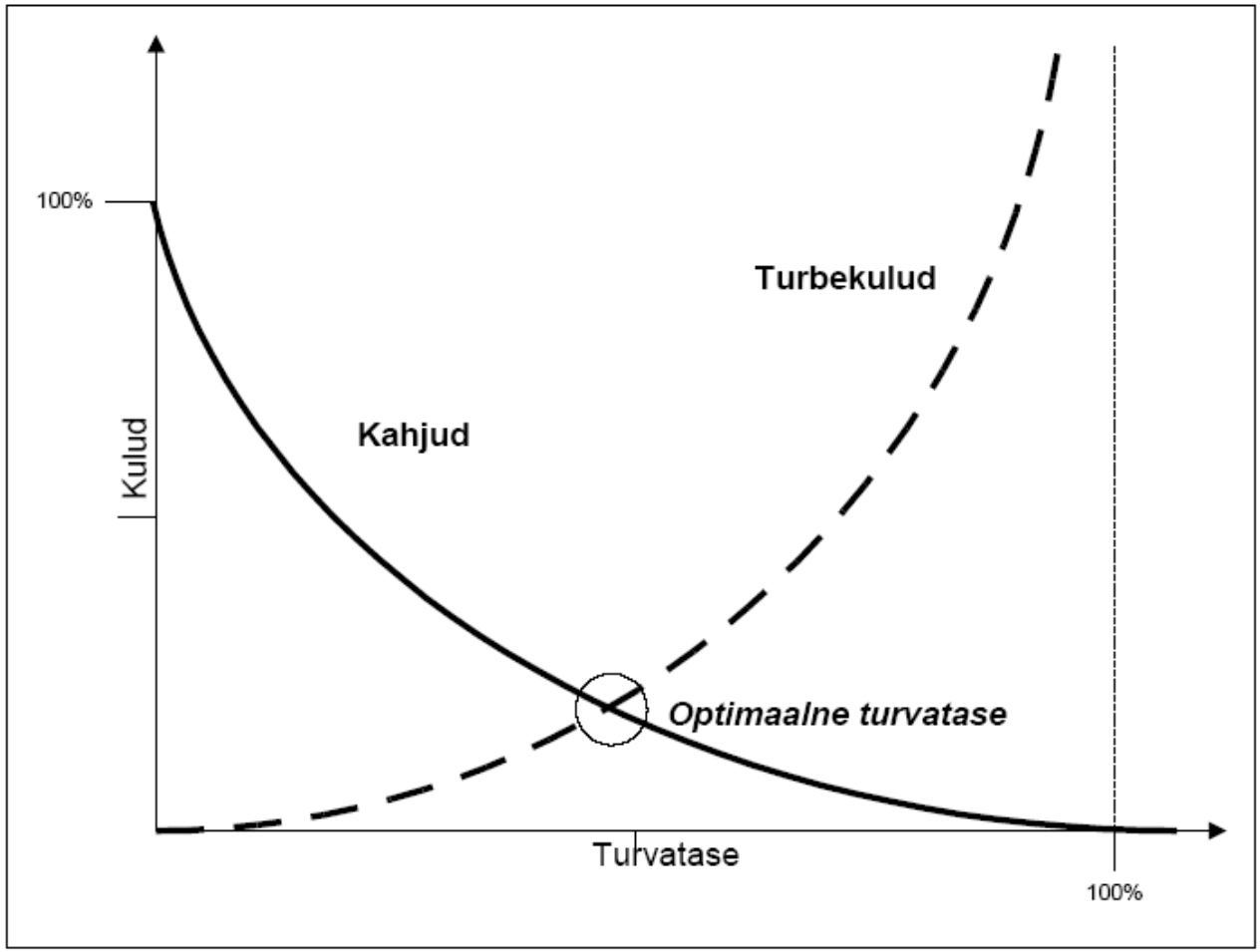
Kahjuks puudub (ilmselt) metoodika, mis määratleks ära potentsiaalsete kahjude ja turvakulutuste vahelise sõltuvuse.

Kuid sellelt jooniselt on selgelt näha ühe ikka veel küllalt levinud arusaama (nõude) ebaotstarbekus - infoturbes on üritus (nõue) turvaintsidentide ja neist tingitud kahjude välistamiseks majanduslikust optimaalsusest väga kaugel.

Veel üks huvitav ja ootamatu tulemus** (kui joonisel kujutatud sõltuvused paika peavad)**:
turvakulutused minimaalsed ja majanduslikult optimaalsed punktis, kus turvaintsidentidest tingitud kahjud ≈ infoturbe kulutustega.

Analoogne pilt raamatust INFOSÜSTEEMIDE TURVE I ,TURVARISK

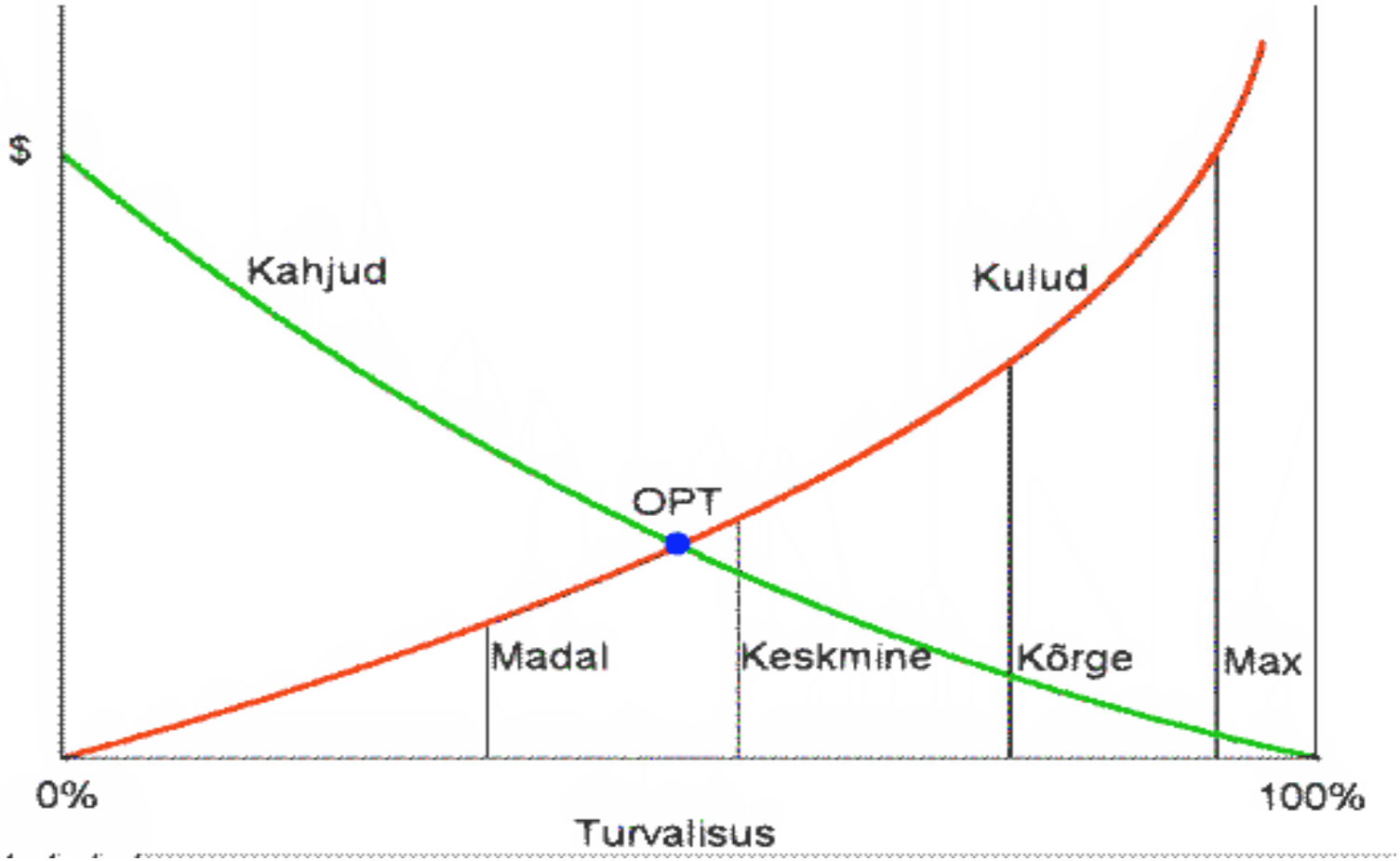
Vello Hanson, Ahto Buldas, Tarvi Martens, Helger Lipmaa, Arne Ansper, Viljar Tulit



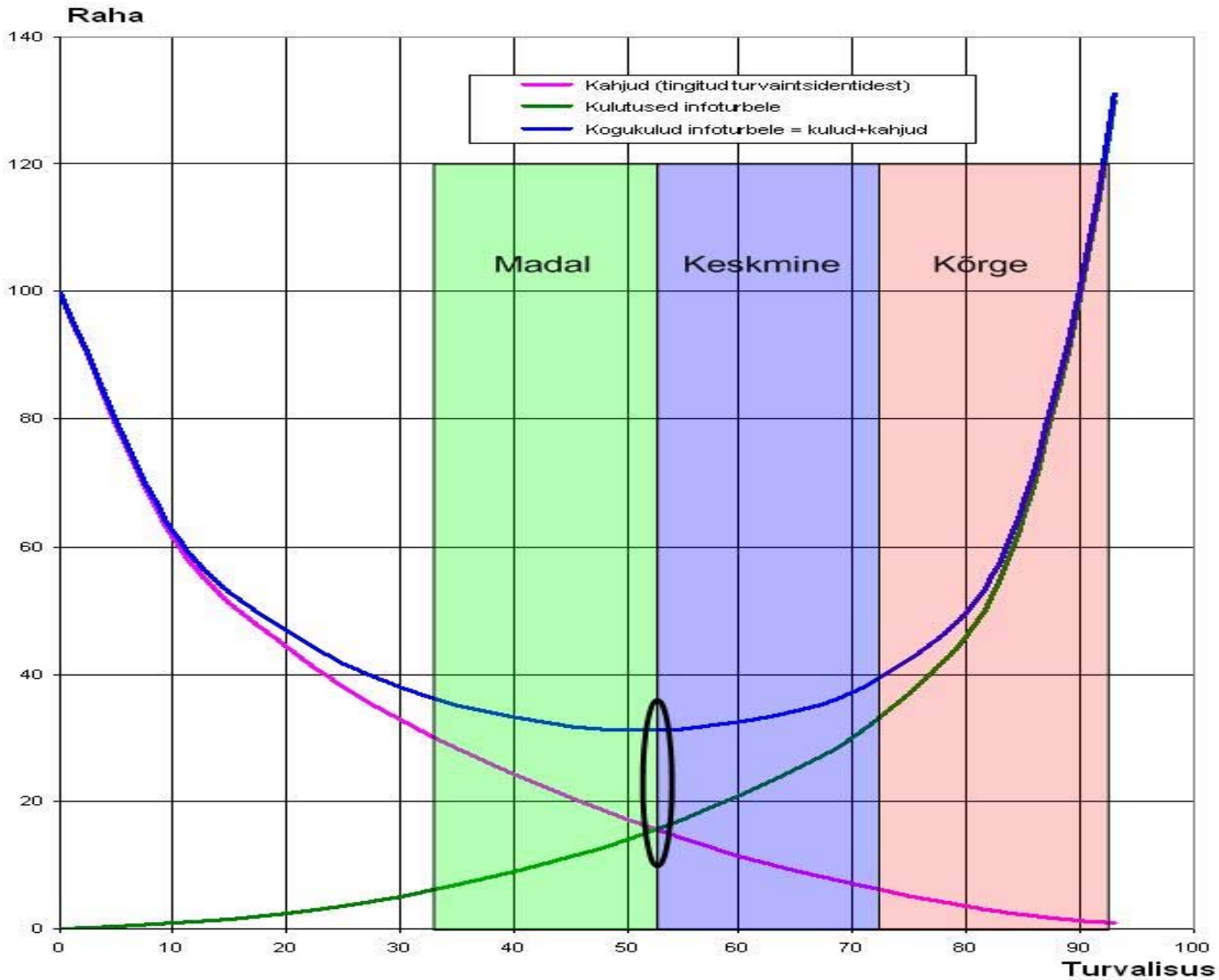
Joonis 6. Kahjude ja turbekulude tüüpiline sõltuvus turvatasemest

Turvatase = Tõrjutud ründed / Kõik ründed ???

Ja ilmselt eelmise joonise baasil tehtud Valdo Prausti versioon – sisse on toodud ISKE madal/keskmine/kõrge-turvatasemed:



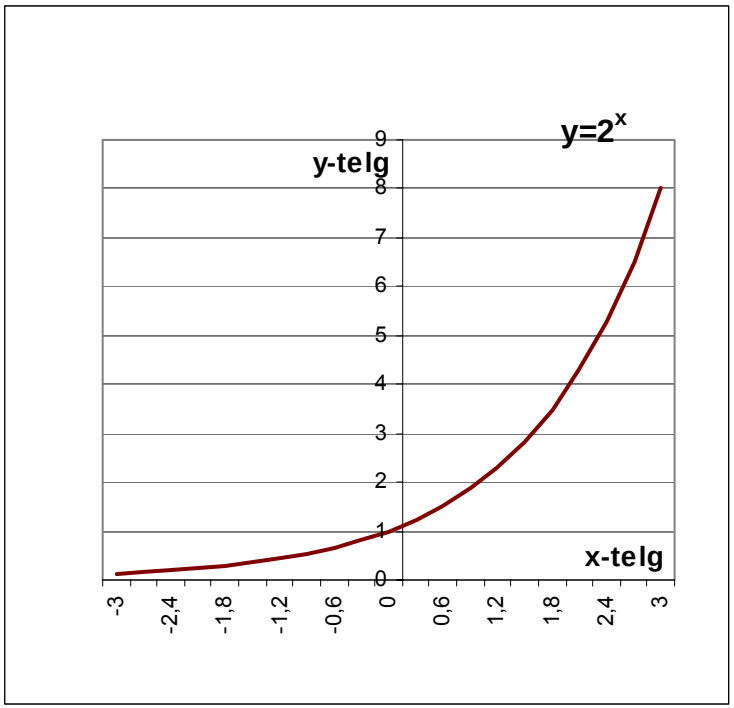
Optimaalne turvatase / optimaalsed infoturbekulutused

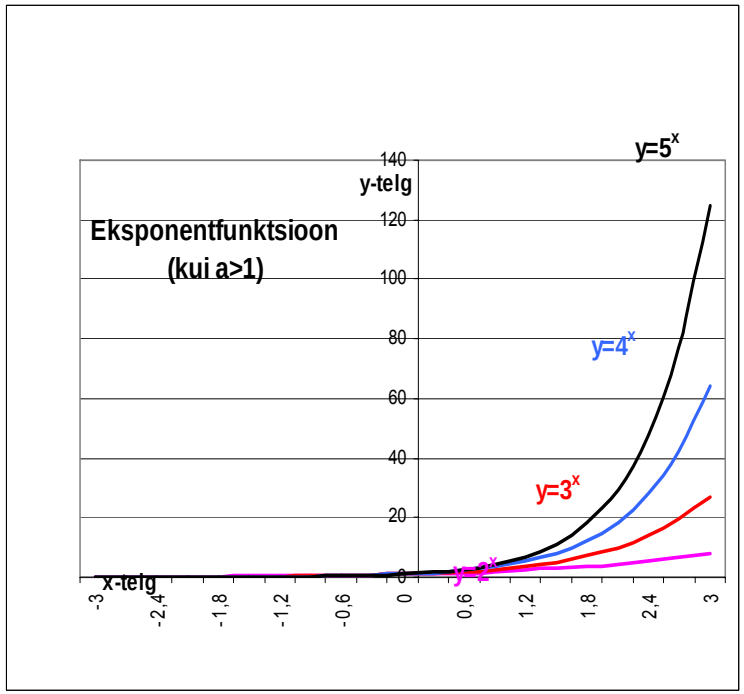


Edasi püüan määratleda optimaalsuse koha sõltuvust info väärtusest.

Alustuseks tuleks seni käsitletud kõverad esitada matemaatiliste funktsioonidena.

Milline näiteks turvakulutuste ja turvataseme sõltuvus võiks välja näha?
Esimene mõte -> eksponentfunktsioon?





$y = 2^x - 1$?
$y = e^x - 1$?

Seega eksponentfunktsioon pole just eriti sobiv.

Kui häda suur, siis abi vägagi tihti osutub olevat küllaltki lähedal.

Täitsa juhuslikult sattusin kokku olemuselt samalaadset probleemi käsitlenud prantsuse bioloogi, Nobeli preemia laureaat Jacques Monod, nn Monod' kasvufunktsiooniga - bakterkultuuride kasvu-kiiruse sõltuvus toidu hulgast.

The Growth of Bacterial Cultures, Jacques Monod (1910-1976),
Annual Review of Microbiology, October 1949, Vol. 3, Pages 371-394

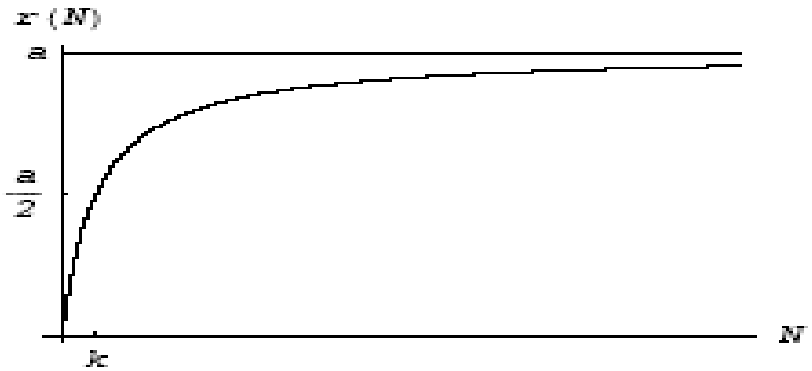
Jacques Monod (1910 - 1976)
received the Nobel Prize in Physiology or Medicine (1965) for his work on the regulation of the *lac* operon (with François Jacob).
While best known as a biochemist, Monod was also well respected for his many articles on politics and philosophy.

Tema poolt käsitletud probleemi loogika ja vastav matemaatiline funktsioon/seda kujutav kõver tundusid vägagi sarnane olevat meie andmeturbe kulutuste ja nendega saavutatava turvataseme omaga.

Monod käsitleb piiratud toitainete koguse korral populatsiooni kasvu kiirust (growth rate). Bioloogias kasutatakse tihti terminit kasvu kiirus ühe isendi kohta (growth rate per capita) r . Olgu toiteainete kontsentratsioon N . Siis r(N) antakse nn Monod' kasvufunktsiooniga:

$$r(N) = a\frac{N}{k+N}, \qquad N \geq 0,$$

ja kus a ja k on konstandid ning ka > 0.



Populatsiooni paljunemiskiiruse sõltuvus toitainete kontsentratsioonist.

Graafikult on näha, et kontsentratsiooni N kasvamisel läheneb kasvukiirus konstandile a: r -> a, st a on populatsiooni kasvukiirus nn küllastustasemel - toitainete hulga kasvamisel populatsiooni kasvukiirus ei suurene enam oluliselt.

Juhul, kui toitainete kontsentratsioon on saavutanud taseme N = k, siis r(N) = a/2 – st populatsiooni kasvukiirus on saavutanud poole küllastustaseme kasvust. Seetõttu nimetatakse konstanti k poolküllastuskonstandiks.

Monod Growth Kinetics

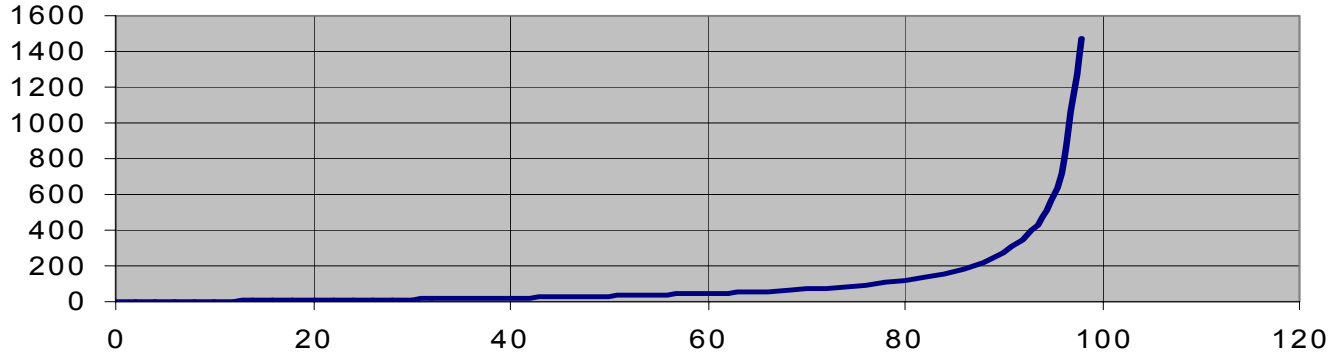
- Relates specific growth rate, μ, to substrate concentration S
- Empirical---no theoretical basis—it just “fits”!
- Have to determine μ_{max} and K_s in the lab
- Each μ is determined for a different starting S

$$\mu = \frac{\mu \max S}{Ks + S}$$

Monod' kasvufuntsiooni viimine meid konkreetselt huvitavatele kujudele:

1. Turvakulutuste kõver

Monod' st kui x<->y: $y_1=k_1x/(a_1-x)$;
ning kuna maksimaalne turvatase $a_1=100$ ning
kui poolküllastuskoefitsient võtta=15, siis $y=15x/(100-x)$.

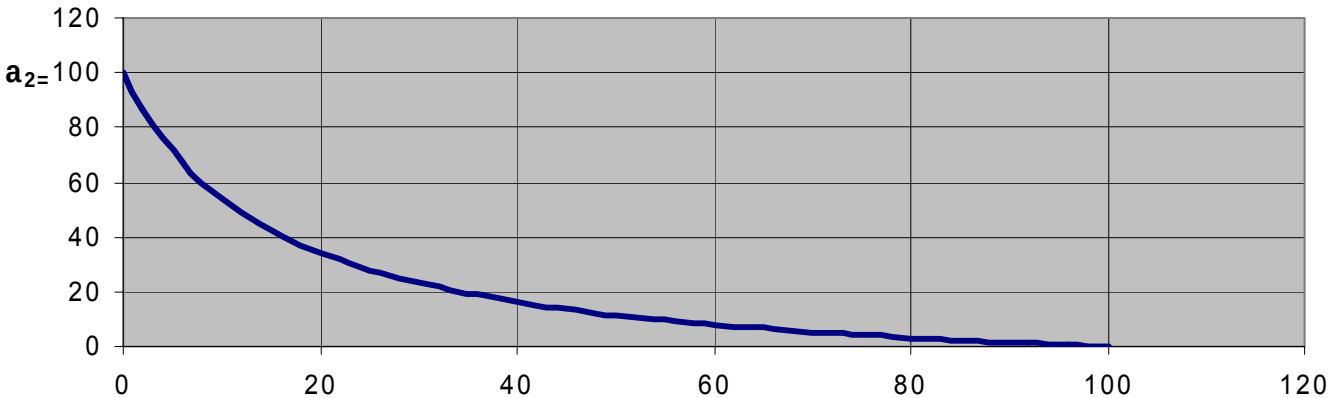


2. Turvakahjude kõver

Pööratud Monod': $y_2 = a_2 - a_2x/(k_2+x)$

+ viia see kujule, et x=0 juures $y=a_2$ ning $x=a_1=100$ juures y=0, siis

$y_2=a_2k_2(a_1-x)/a_1(k_2+x)$ ja (a1=a2=100 ning k2=15) **$y_2=15(100-x)/(15+x)$**



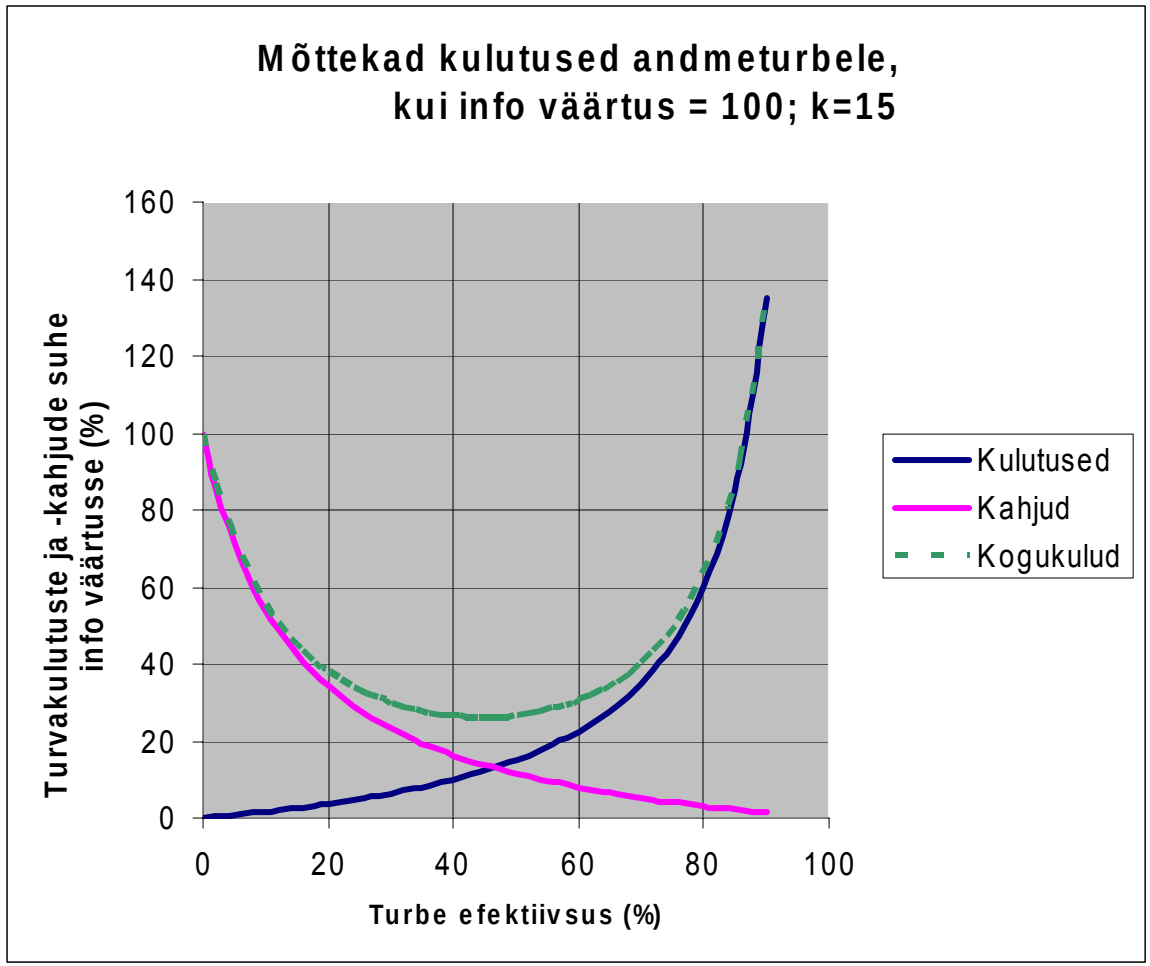
Kui hakata Monod' kasvufuntsioonist üle minema infoturbe kulutuste ja kahjude turvalisusest sõltuvuste funktsioonide kujutamisele, siis on ainult üks probleem –
tuleb määratleda Monod' konstantide "a" ja "k" vasted:

1. **Väga lihtne on Monod' "a"-ga:**
   - kulutuste korral on selleks maksimaalne (100%) turve,
   - kahjude korral on selleks maksimaalne (100%) kahju
   ja max kahju = info väärtusega.
2. **Veidi keerukam on lugu "k"-ga – nn poolküllastuskonstant määratleb siin raha millega saavutatakse ~50%-ne turvatase.**

Reaalne on "k" vahemikus 5 – 25
(st praktikas kulutused infoturbele ligikaudu selles vahemikus) :

- **k = 5 korral on optimaalsed kulutused ~5% info väärtusest**
- **k=10 korral on optimaalsed kulutused ~9% info väärtusest**
- **k=15 korral on optimaalsed kulutused ~13% info väärtusest**
- **k=25 korral on optimaalsed kulutused ~20% info väärtusest**

Edaspidi võtan aluseks keskmise k=15.


Mõttekad kulutused andmeturbele,
kui info väärtus = 100; k=15
Turvakulutuste ja -kahjude suhe info väärtusse (%)
160
140
120
100
80
60
40
20
0
0
20
40
60
80
100
Turbe efektiivsus (%)
Kulutused
Kahjud
Kogukulud

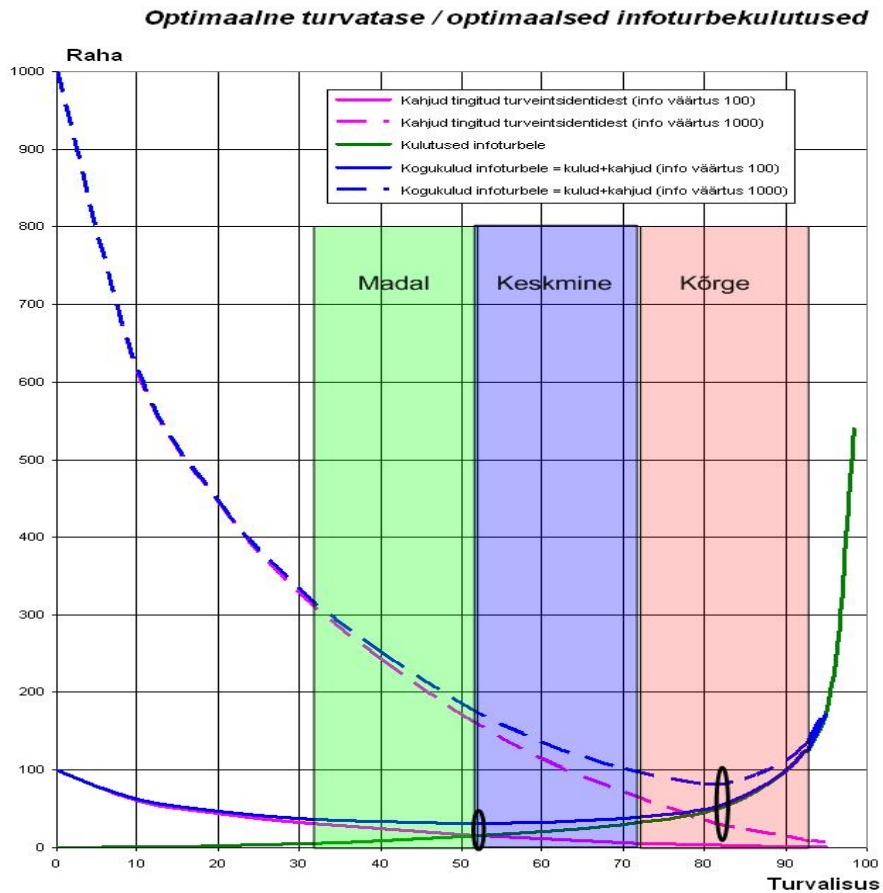
Milleks nende turbe kulutuste/kahjude kõverate matemaatiliste kujude saamine üldse oluline ja hea on?

1.
Eelmisel slaidil esitatud jooniselt on näha, et optimaalsuspunktis on infoturbe kulutused ja ka kahjud ~13% info väärtusest.

Seega keskmiselt heade turbe lahenduste korral on andmeturbe kulutused minimaalsed/optimaalsed kui turvatase 44,5% ja optimaalsed kulud andmeturbele on ~26% info väärtusest – st kulutused ~13% ja kahjud ~13% (NB! kui k=15).
(vt Äripäeva "IT juhtimise käsiraamatu" artiklit "10.5.7. Mõttekad kulutused infoturbele")

2.
Info väärtuse 10x kasvu puhul:

- optimaalsuspunkt nihkus madala-keskmise taseme piirilt selgelt kõrgesse,
- info väärtuse 10x kasvu korral mõttekad kulutused kasvasid ~3x,
- info väärtust mitte arvestades pole erilisi lootusi infoturbe kulutuste optimaalsuse tagamiseks.

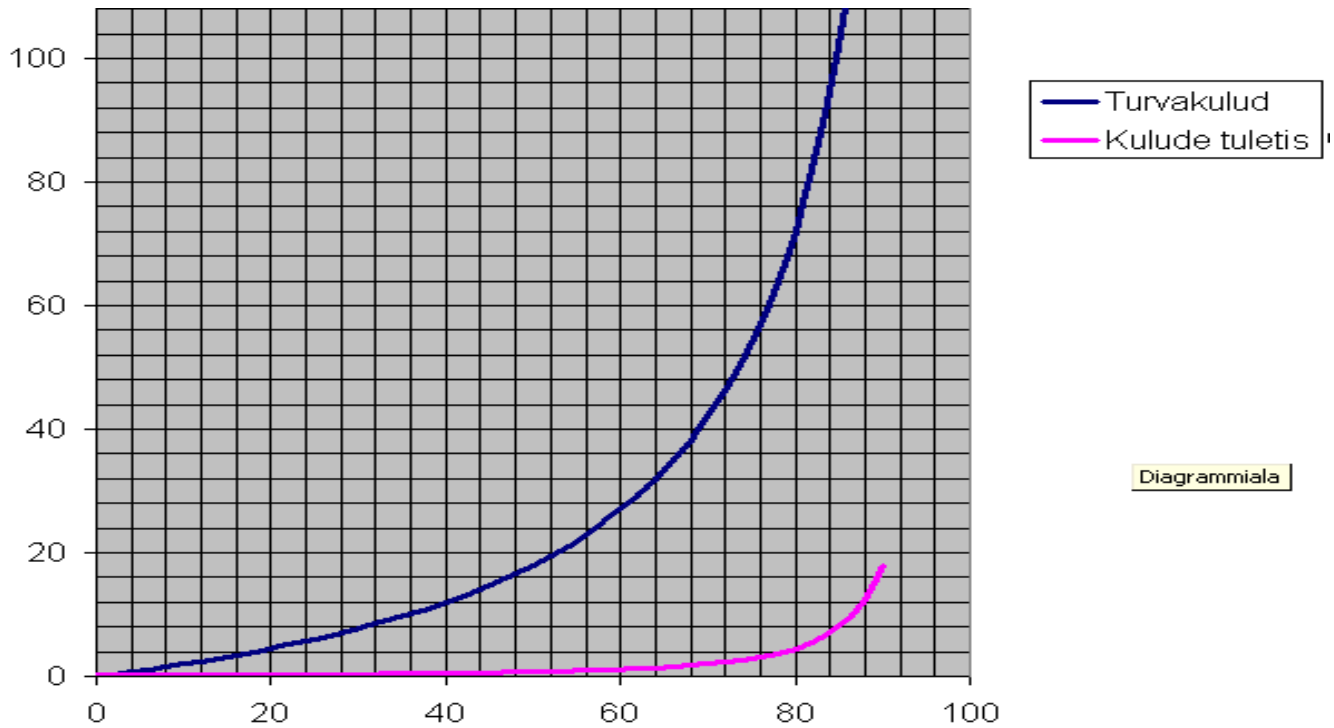


3.
Return of Investments

Turvakulutused $y=k_1x/(a_1-x)$

(**konkreetselt y=18x/(100-x)**)

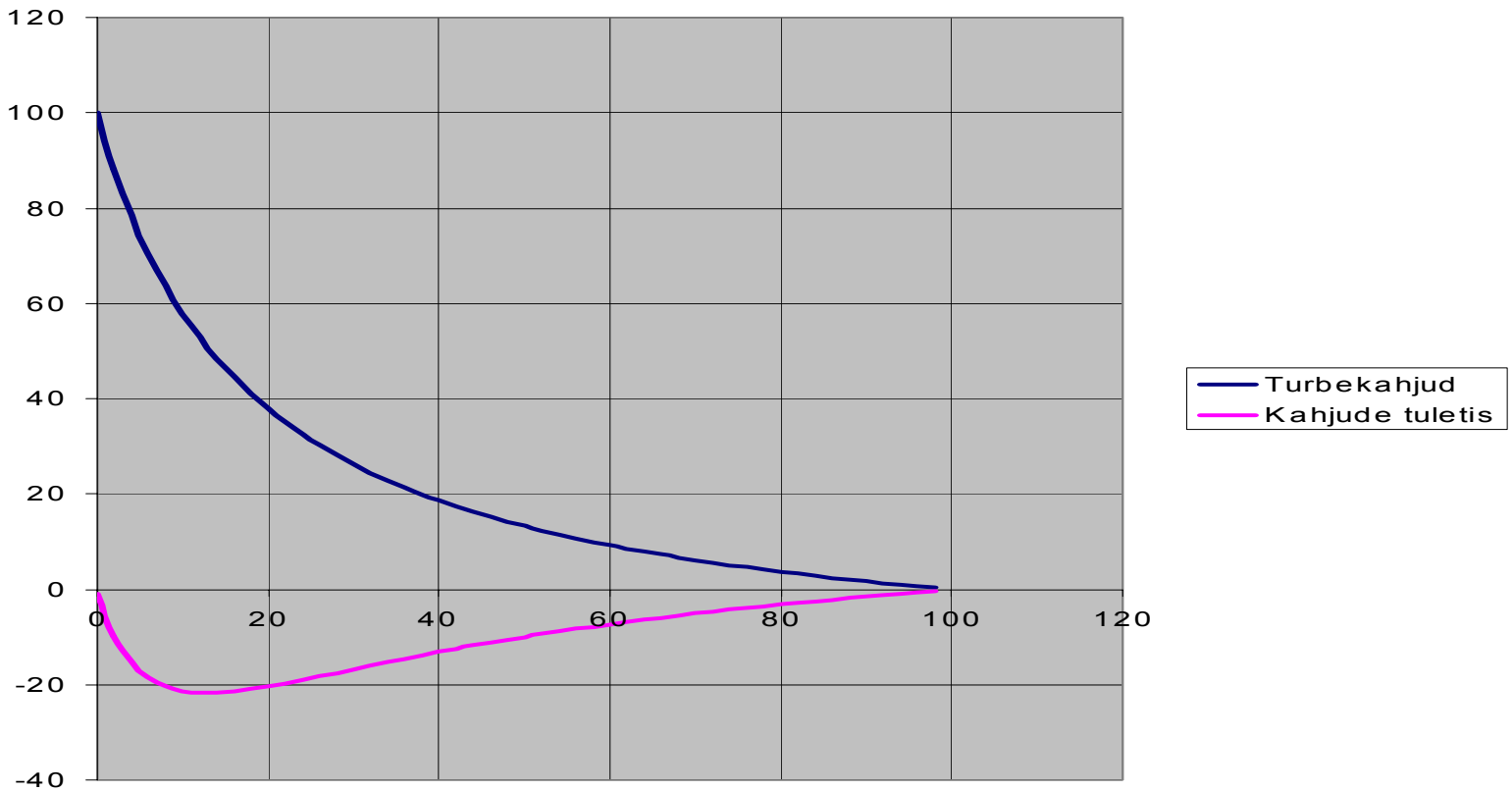
ja selle tuletis $y' =1800/(100-x)^2$

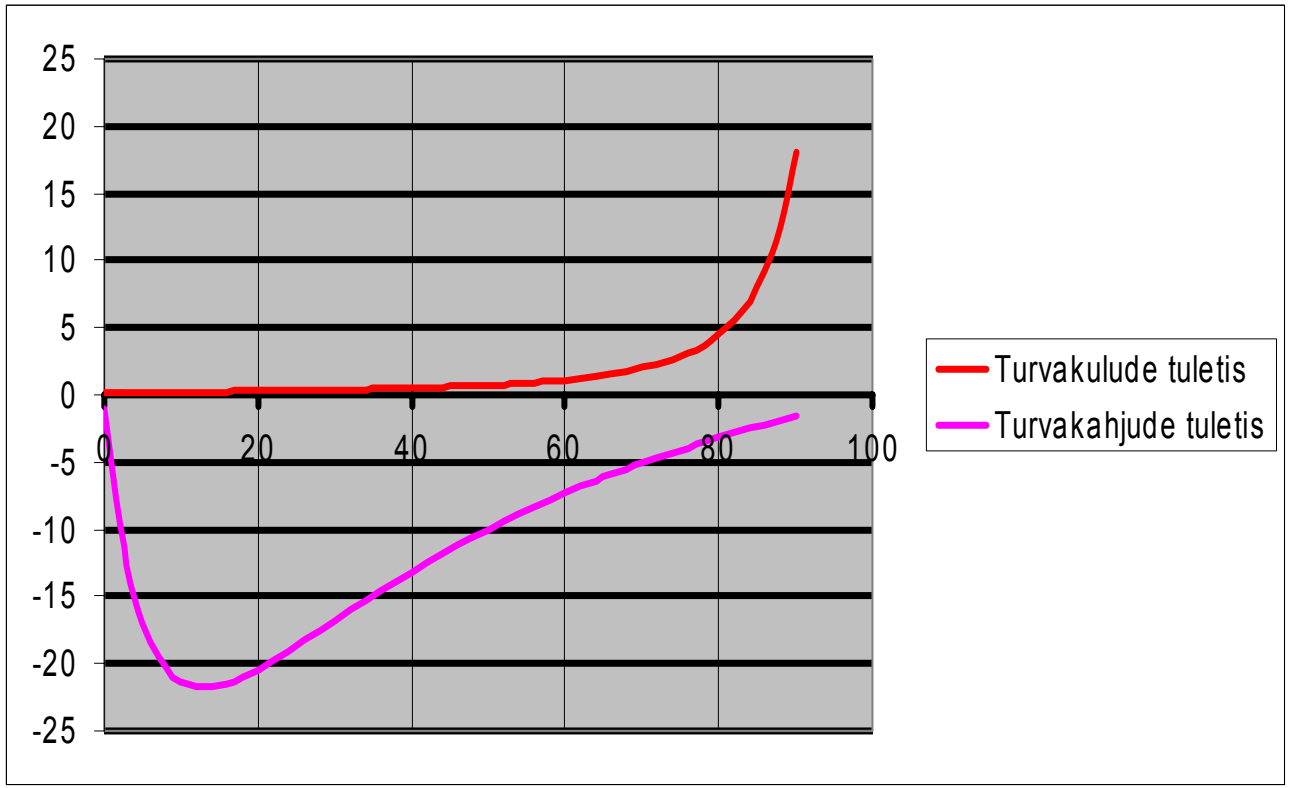


Turbekahjude funktsioon $y=a_2k(a_1-x)/a_1(k+x)$

(konkreetselta$_2$=a$_1$=100 ja k2=18: $y=18(100-x)/(18+x)$)

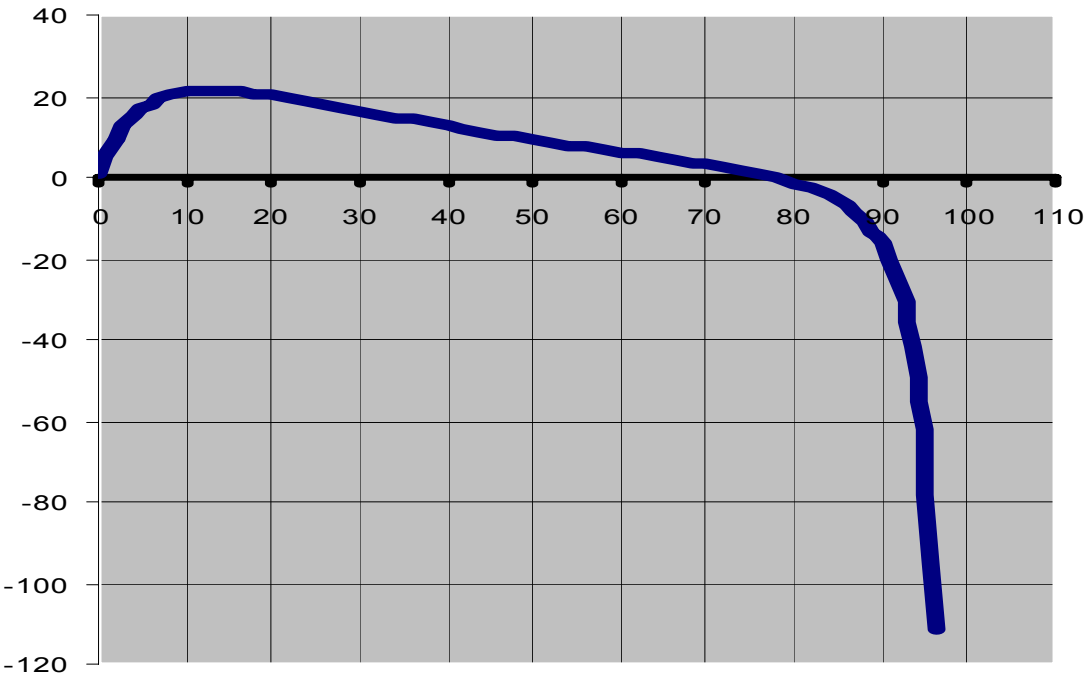
ja selle tuletis $y' = 18(x^2-101x-18)/(x+18)^2$.




25
20
15
10
5
0
-5
-10
-15
-20
-25
0
20
40
60
80
100
Turvakulude tuletis
Turvakahjude tuletis

Positiivse RoI – piirkond kui a_2=100:

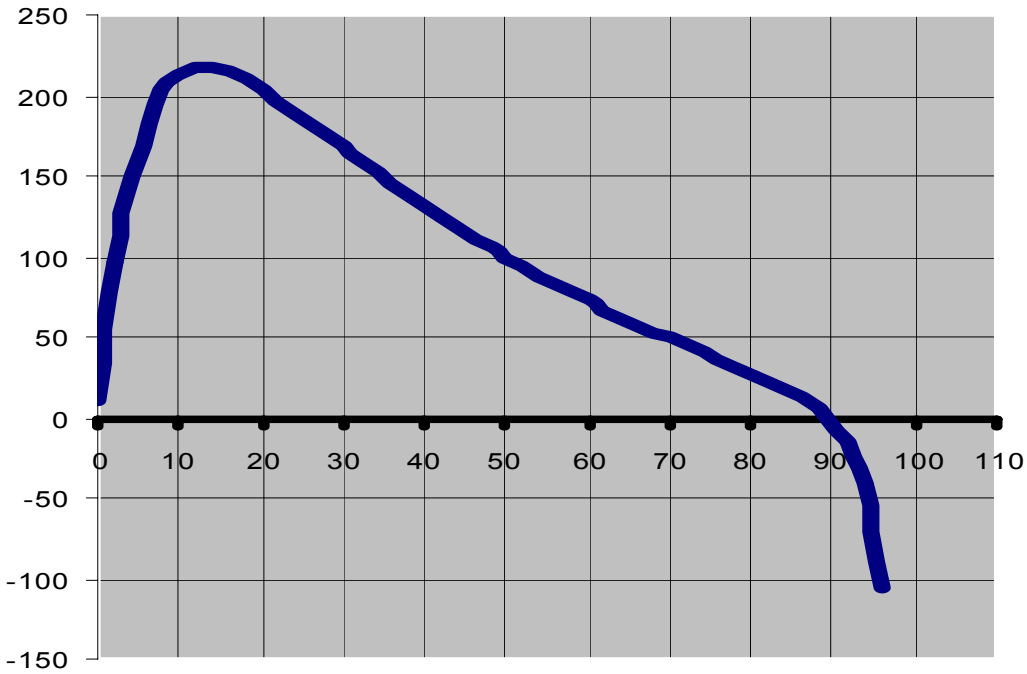
turvakahjude ja turvakulutuste tuletiste vahe >0



RoI positiivne piirkonnas, kus turvakahjude kahanemine on kiirem kui turvakulutuste kasv, st kahjude tuletis suurem kulutuste tuletisest, ja nagu jooniselt näha on selleks efektiivsuse vahemik 0 ÷ 75.

Positiivse RoI – piirkond kui a_2=1000:

turvakahjude ja turvakulutuste tuletiste vahe >0



RoI on positiivne piirkonnas, kus turbe efektiivsus 0 ÷ 90.

2. metoodika

Üldprintsiip – **määratleda mõistlike kulutuste suurus kaitstava info väärtuse kaudu.**

Info väärtust võib esimeses lähenduses määratleda kui nõutava konfidentsiaalsuse-, käideldavuse- ja tervikluse taseme mittetagamisel asutuse vastava funktsiooni (korrektsest) mittetäitmisest tingitud võimalikud potentsiaalsed kahjud (saamata jäävad tulud, võimalikud leppetrahvid jms). Lõplikul/täpsemal infovara väärtuse määratlemisel lisanduvad veel kulutused taastamisele, moraalne kahju jms.

Ja kohe ka selle metoodika teine suur mõte: äriinfo turvanõudeid ja nende mittetäitmisest tingitud võimalike potentsiaalseid ärilisi kahjusid suudavad hinnata vaid asutuse äripoole esindajad – **seega mõttekad kulutused infoturbele määratleb äripool ise**.

Ning lisaks veel üks tähelepanek: riigiasutustel on üldjuhul küllalt raske rahas mõõta saamata jäänud tulusid ning otstarbekam on info väärtust määratleda kulupõhiselt – st info väärtus ≈ kulutustega selle info saamiseks/töötlemiseks.

Soovitud reaalsete mõttekate infoturbe kulutusteni jõudmiseks pakun välja kolm võimalust:

1. **Leida riskid (määratleda tõenäosused potentsiaalsete kahjude tekkimiseks) ja andmeturbe kulud < turvaintsidentide läbi tõenäoliselt tekkivad kahjud**

2. **Kuid võiks lähtuda ka konkreetsest situatsioonist – infot on vähevõitu ja ka olemasolev on suhteliselt ebatäpne ning tegutseda edasi analoogselt üldlevinud kindlustus-põhimõtetega – a'la esialgsed mõttekad kulutused (uus infosüsteem) oleksid näiteks info väärtusest ~10÷20% ning edasi ~5 ÷ 10% aastas.**

3. **Tundub, et veel paremate/täpsemate tulemusteni jõuab, kui võtta arvutustes aluseks eelmise aasta andmeturbe kulutuste (eeldades näiteks, et eelmisel aastal olid andmeturbe kulutused normaalsed - st olulisi infoturvaintsidente polnud) ja info väärtuste suhte.**

1. **Leida riskid (määratleda tõenäosused potentsiaalsete kahjude tekkimiseks)**

   ja

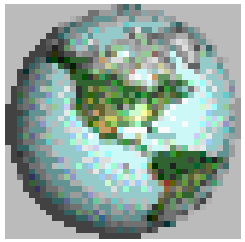
   andmeturbe kulud < turvaintsidentide läbi tõenäoliselt tekkivad kahjud

- Leiame riskid $r_i = P_i \cdot K_i$

  Riskina mõistame me ebasoovitava sündmuse ilmnemist.
  Riski iseloomustavad tõenäosus ja mõju - seega on riski rahaline väljendus funktsioon ebasoovitava sündmuse tõenäosusest ja sündmusega kaasnevast kahjusummast.

  Infosüsteemide riskianalüüsis tuleb tegelikult riske tunduvalt täpsemalt kirjeldada/käsitleda.

  Alustuseks näiteks, et riske hinnates annab ebasoovitavate sündmuste esinemise tõenäosuste asemel nende esinemissageduse kasutamine jupi paremini arusaadava pildi potentsiaalsetest probleemidest ja kahjudest.



Обобщенный критерий информационной безопасности АБС

(из методики французской банковской комиссии)

$$R = \sum_{i=1}^{n} (A_i \cdot B_i + C_i) < R_{\max}$$

R-суммарные издержки
n-количество рисков
A-вероятный риск
B-стоимостная оценка риска
C-стоимость реализации мер защиты
Rmax-оценка допустимого риска

Analysis of the System -- Effectiveness Equation

Force Protection

- Effectiveness = P_A * [1 – (P_I * P_N)] * C
  - Is the current system effective – can we accept the level of effectiveness
  - Can we improve the system – at what cost

P_A = Probability of Attack
P_I = Probability of Interruption
P_N = Probability of Neutralization
C = Consequence

Turvanõuete/turvaosaklasside määratlemine (Eesti riigiasutuste ISKE):

Teabe hilinemise tagajärgide lubatav kaalukus (R):

R0 - teabe saamata jäämisega ei kaasne olulisi tagajärgi;
R1 - andmete saamata jäämine põhjustab häireid riigikorralduses või asutuse tegevuses, ohtu inimeste tervisele või keskkonnasaaste ohtu;
R2 - andmete saamata jäämine põhjustab olulist kahju riigi suveräänsusele, ohtu inimelule või keskkonnasaastet;
R3 - andmete saamata jäämine põhjustab suveräänsuse kaotamise ohtu, mitmeid hukkunuid või ulatuslikku keskkonnasaastet.

Aegkriitilise teabe käideldavus (K):

K0 - teabe saamisele ei ole seatud tähtaegu;
K1 - teabe saamisele on seatud tähtaeg päevades;
K2 - oluline on teabe saamine tundide jooksul;
K3 - oluline on teabe saamine sekundite jooksul.

Teabe terviklus (T):

T0 - teabe allikas ega muutmise tuvastavatus ei ole olulised;
T1 - teabe muutmise fakt peab olema tuvastatav;
T2 - teabe allikas peab olema tuvastatav;
T3 - teabel on tõestusväärtus.

Teabe konfidentsiaalsus (S):

S0 - juurdepääsu teabele ei piirata;
S1 - teabele juurdepääsu tingimuseks on juurdepääsu taotleva isiku identifitseerimine;
S2 - juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;
S3 - teave on seaduse alusel tunnistatud juurdepääsupiiranguga teabeks.

Infoturbenõuete standardvorm (vastavalt turvaalase klassifitseerimise üldpõhimõtetele EÜPs).

Infovara nimetus : ..... *Valdaja :* .....

Infoturbe nõuded		Selgitus	x / - (jah/ei)	Infoturbe klassifikaator	Infovara väärtus (= võimalikud kahjud miljonites EEKides/aastas) *
Konfidentsiaalsuse nõuded		**Avalikud andmed.**		S0	
		Andmed sisemiseks kasutamiseks - andmete avalikustamine võib põhjustada materiaalset või moraalset kahju		S1	S1⇒S0
		Salajased andmed - andmete avalikustamine häirib Panga funktsioneerimist või rikub inimese privaatsust.		S2	S2⇒S1
					S2⇒S0
		Eriti salajased andmed - andmete avalikustamine on ohtlik Panga või inimese julgeolekule, võib põhjustada kontrollimatuid muutusi Panga tähtsates süsteemides.		S3	S3⇒S2
					S3⇒S1
					S3⇒S0
Käideldavuse nõuded	Aegkriitilisus *	Andmed, mille hilinemine ei põhjusta komplikatsioone.		K0	
		Andmed, mille mõnepäevane hilinemine ei põhjusta komplikatsioone.		K1	K1⇒K0
		Andmed peavad olema kättesaadavad mõne tunni jooksul. Info kättesaamine vajalik/nõutav (arvestame ainult kahe praktikas enamlevinud ohukorraga): kas katkematult – st 7x24h või ainult tööajal – st 5x8h.		K2 .... x	K2⇒K1 K2⇒K0
		Andmed tuleb saada üldjuhul mõne sekundi jooksul, kuid mõneminutised tõrgetest/riketest põhjustatud katkestused sagedusega ~ kord päevas ei põhjusta ohuliselt ebasoovitavaid probleeme. Info kättesaamine vajalik/nõutav (arvestame ainult kahe praktikas enamlevinud ohukorraga): kas katkematult – st 7x24h või ainult tööajal – st 5x8h.		K3 .... x	K3⇒K2 K3⇒K1 K3⇒K0
	Hilinemise tagajärgede kaalukus	Andmete õigeaegne mittesaamine ei too kaasa mainimisväärseid tagajärgi.		R0	
		Andmete õigeaegne mittesaamine võib põhjustada takistusi Infosüsteemi funktsiooni (ja vastava Panga funktsiooni) täitmiseks.		R1	R1⇒R0
		Andmed, mille õigeaegne mittesaamine toob kaasa ohulisi takistusi Infosüsteemi funktsiooni (ja vastava Panga funktsiooni) täitmiseks.		R2	R2⇒R1
					R2⇒R0
		Andmete õigeaegne mittesaamine toob kaasa Infosüsteemi funktsiooni (ja vastava Panga funktsiooni) mittetäitmise.		R3	R3⇒R2
					R3⇒R1
					R3⇒R0
Tervikluse nõuded	Andmeallika / muutja tuvastatavus	Andmete sisestaja/muutja tuvastatavus pole oluline		T0	
		Andmed, mille volitamatud muutmised peavad olema tuvastatavad (seda ka juhul, kui need on tehtud süsteemiülema poolt tematöö käigus).		T1	T1⇒T0
		Andmed, mille allikas peab olema tuvastatav. (Siia kuuluvad andmed on piisava tähtsusega, mistõttu peab vastutav töötleja saama tuvastada, kes on andmed sisestanud või neid viimati muutnud.)		T2	T2⇒T1
					T2⇒T0
		Andmed, mille allikat peab saama tõestada kolmandale osapoolele. (Siia kuuluvad andmed on sedavõrd kaaluka tähtsusega, et nende sisestajat või viimaste muudatuste tegijat võib olla vaja kohtus tõestada.)		T3	T3⇒T2
					T3⇒T1
					T3⇒T0

* **Infovarade väärtus** määratletakse esimeses lähenduses kui nõutava konfidentsiaalsuse-, käideldavuse- ja/või tervikluse taseme mittetagamisel Panga vastava funktsiooni (korrektsest) mittetäitmisest tingitud võimalikud kahjud (saamata jäävad tulud, võimalikud leppetrahvid jms). Lõplikul/täpsemal infovara väärtuse määratlemisel lisanduvad veel kulutused taastamisele.
Võimalike kahjude määratlemisel pakuks algvariandiks välja vahemikud:

- alla 100 000 EEKi/aastas
- 100 000 kuni 1 000 000 EEKi/aastas
- 1 000 000 kuni 10 000 000 EEKi/aastas
- 10 000 000 kuni 100 000 000 EEKi/aastas

** Kõrgemate käideldavusnõuetega süsteemide puhul on turvameetmete (põhiliselt Talitluspidevuse- ja taasteplaanide osas) määratlemise seisukohalt väga oluline, millal esitatud nõue peab täidetud olema. Piirdume esialgu kahe olulisema variandiga – kas pidevalt - st **7 x 24** või ainult tööajal – st **5 x 8** .

Panga infosüsteemide spetsiifikast tingitud täiendavad turvanõuded:

- Tervikluse osas on lisaks tuvastatavusele küllalt tihti sama oluline ka andmete/muutmiste õigsus ja täielikkus - seega võivad olla vajalikud spetsiaalsed andmete õigsuse ja täielikkuse kontrollid (enne andmete kasutamist, perioodilised päeva- ja kuulõpu protseduurid, vms).

Infoturbe nõuded		Selgitus	x / - (jah/ei)	Infoturbe klassifikaator	Infovara väärtus - võtakse võrdseks võimaliku kahjuga (miljonites EEKides/aastas)
Tervikluse nõuded	Andmete õigsus / täielikkus	Andmete õigsus ja täielikkus pole oluline.		**Õ0**	
		Vajalikud spetsiaalsed perioodilised (kuu, kvartal, aasta) andmete õigsuse/täielikkuse kontrollid.		**Õ1**	**Õ1⇒Õ0**
		Vajalik andmete õigsuse/täielikkuse kontroll iga pangapäeva lõpus.		**Õ2**	**Õ2⇒Õ1** **Õ2⇒Õ0**
		Vajalik jooksev (enne andmete kasutamist) andmete õigsuse ja täielikkuse kontroll.		**Õ3**	**Õ3⇒Õ2** **Õ3⇒Õ1** **Õ3⇒Õ0**

- Võimalikud on täiendavad nõuded infoturbele veel näiteks ka juhtudel kui info kuulub isikuandmete kaitse-, pangandus- või raamatupidamisseaduste mõjusfääri ning seetõttu esitatakse erinõudmisi kontrollidele, arhiveerimisele, deklassifitseerimisele vms.
- Lepingud väliste partneritega (SWIFT, VISA jne) võivad määratleda täiendavaid turvanõudeid.

Täiendavad infoturbe nõuded	Selgitus
……	……
……	……

Valdaja nimi ……

Allkiri ……

Valdajate küsitluse kiire hinnang/analüüs

Kahjud nõutava konfidentsiaalsuse taseme mittetagamisel (miljonites EEKides)				Kahjud nõutava käideldavuse taseme mittetagamisel (miljonites EEKides)				Kahjud nõutava tuvastatavuse taseme mittetagamisel (miljonites EEKides)				Kahjud õigsuse/täielikkuse mittetagamisel miljonites EEKides)	
Langeb ühe taseme		Langeb kaks taset		Langeb ühe taseme		Langeb kaks taset		Langeb ühe taseme		Langeb kaks taset			
min	max	min	max	min	max	min	max	min	max	min	max	min	max
3.1	33.4	282.8	1 223.4	8.0	77.1	141.2	602.1	29.2	292.6	77.3	773.6	83.0	825.4

Valdajate hinnangute põhjal on äriinfo kõige olulisemateks väärtusteks info konfidentsiaalsus ja terviklus, info käideldavuse väärtust hinnati eelnevatest ligi ~2x madalamaks.
Infovarade väärtust määratleme esimeses lähenduses kui nõutava konfidentsiaalsuse-, käideldavuse- ja/või tervikluse taseme mittetagamisel Panga vastava funktsiooni (korrektsest) mittetäitmisest tingitud võimalikud kahjud (saamata jäävad tulud, võimalikud leppetrahvid jms).
Mõttekad kulutused infoturbele on otseselt seotud info ärilise väärtusega – tuleb säilitada tasakaalu äriinfo väärtuse ja turvakulutuste vahel.

Valdajate poolt määratletud äriinfo väärtuste summa, minimaalselt ~600 miljonit ja maksimaalselt ~4 miljardit EEKi, **ületab vähemalt kaks suurusjärku reaalseid eraldusi/kulutusi andmeturbele – st kulutustega liialdatud igal juhul pole.**
Aga ehk pööratakse Ühispangas liiga vähe tähelepanu (ressursse) andmeturbele ?
Või pole päris õige võrrelda maksimaalsete riskidega?
NB!!! Järgmiseks infovaldajate küsitlemiseks vaja täpsustada info väärtuse määratlemise metoodikat.

Äripool määratleb suurepäraselt nõutava turvataseme ja selle mittetäitmisest põhjustatud potentsiaalsete kahjude ***suurusjärgu*** (küllalt tihti ka täpsemalt) turvanõude taseme täpsusega.

Näiteks kahjud ülisalajase info lekkimisel panga siseselt (S2->S1) ja pangast välja (S2->S0).

Tõenäosustele suudab äripool suurepäraselt teha kolmetasemelise High-Middle-Low määratlemise. Ehk ka viietasemelise.

Kuid selle metoodika täpsuseks jääb ligikaudselt suurusjärk (eriti täpsemad äripoole eksperthinnangud lihtsalt pole).

Kui tegelikkuses pole võimalik määratleda asutuse info väärtusele selliseid objektiivseid omadusi nagu näiteks hind (ja riigi- ning sõjaväe asutustel see üldjuhul nii ongi), siis peame leppima riskihinnangutega teenuse osutamise raskendatuse/võimatuse tasemetega või siis abi otsima analüütlisest hierarhiaprotsessist ning Saaty meetodist/skaalast (vt slaidid 47 ÷ 50).

2. Kuid võiks lähtuda ka konkreetsest situatsioonist – infot on vähevõitu ja ka olemasolev on suhteliselt ebatäpne.

Ja tegutseda edasi analoogselt üldlevinud kindlustus-põhimõtetega – a'la esialgsed mõttekad kulutused (uus infosüsteem) oleksid näiteks info väärtusest ~10÷20% ning edasi ~5 ÷ 10% aastas.

Turbe tasuvust võib mõõta valemiga (Noor et al. 2002, 5):

Tasuvus (ROI) = risk ($) / (turbekulutused ($) + jääkrisk ($)) **ehk**

Tasuvus (ROI) = risk ($) / (turbekulutused ($) + (1 – turbe efektiivsus) x risk ($)).

Kui turbe tasuvus on suurem kui 20, siis on see maailmaklassist (Noor et al. 2002, 5).

Noor, I., Joyner, T., Martin, R. J. Jr. 2002.
Challenges of implementing risk management processes.
AACE International Transactions, RISK.04.1-RISK.04.6. ProQuest (online database)
http://www.proquest.com/ (05.05.2004).

Oleks äärmiselt huvitav näha reaalsete kindlustusfirmade reaalseid infosüsteemide infoturbe kindlustuslepinguid.

Eesti kindlustusfimad sellist teenust ei osuta, kuid USA's/Lääne-Euroopas pidavat see küllaltki levinud olema.

Once the risk mitigation plan has been developed, the cost of each step of the risk mitigation plan is determined. The total cost of the risk mitigation plan is obtained by summing the costs of the individual steps of the plan. The cost of executing the risk mitigation plan can be compared to the risk impact costs to determine the return on investment (ROI), as can be seen from equation 1.

$$\text{Return on investment (ROI)} = \frac{\text{risk impact (\$)}}{\text{mitigation costs (\$)} + ((100 - \text{ME}) \times \text{risk impact (\$)})}$$

(equation 1)

In equation 1, the ROI is computed by comparing the risk impact to the total cost of the risk. The total cost of the risk is the mitigation cost plus the unmitigated risk impact. The unmitigated risk impact is computed from the mitigation effectiveness (ME) and the risk impact. If the ME for a risk mitigation plan is 90% and the risk impact is $100,000, then 10% of the risk impact ($10,000) is not mitigated. Thus the unmitigated cost ($10,000) has to be added to mitigation costs to determine the total cost of the risk.

Risk management experts have proposed various ROI metrics to assess the effectiveness of risk management programs. Hall [3] proposes an ROI value of greater than 20 as indicative of a risk management program that is approaching world-class status. Currently, ROI metrics are being collected by the SSSPMO on risks that have been successfully mitigated.

3. **Tundub, et veel paremate/täpsemate tulemusteni jõuab, kui võtta arvutustes aluseks eelmise aasta andmeturbe kulutuste (eeldades näiteks, et eelmisel aastal olid andmeturbe kulutused normaalsed - st olulisi infoturvaintsidente polnud) ja info väärtuste suhte.**

   Arvesse tuleks ilmselt võtta ka mingi infoturbe kulutuste üldine kasvutendents (häkkerid muutuvad aina leidlikumateks, kaitse keerukamaks), info väärtuse kasvu ja uu(t)e info(süsteemide) lisandumist.

Ning mõttekad infoturbe kulutused oleksid:

$$\textit{Kulutused}_{\text{infoturbele uuel aastal}} = K_1 \times K_3 \times K_4 \times \text{Äriinfo}_{\text{väärtus uuel aastal}}$$

või

$$\textit{Kulutused}_{\text{infoturbele uuel aastal}} = K_2 \times K_3 \times K_4 \times \text{Kulutused}_{\text{infoturbele eelmisel aastal}},$$

kus

$K_1 = \text{Kulutused}_{\text{infoturbele eelmisel aastal}} / \text{Äriinfo}_{\text{väärtus eelmisel aastal}}$

$K_2 = \text{Äriinfo}_{\text{väärtus uuel aastal}} / \text{Äriinfo}_{\text{väärtus eelmisel aastal}}$

K_3 = infoturbe kulutuste kasvutendents

K_4 – süsteemide kasvutendents (uute süsteemide lisandumine)

Eksperthinnanguna pakun, et nende metoodikate abil võib jõuda ka kuni 10÷20% täpsuseni.
Kuid seda eeldusel, et meil on olemas mõnede eelmiste aastate korrektsed andmed ja nendest saadud kahjud/koefitsiendid peavad paika ka tulevikus.
St tegemist on suuresti ikkagi nn tagantjärele tarkusega.

Täpsustamistega on võimalik ka edasi minna - määratleda majanduslikult mõttekad kulutused turbevaldkondade lõikes. See tähendaks näiteks info konfidentsiaalsuse, käideldavuse ja tervikluse väärtuste määratlemist.

Ning edasi võib veel käsitleda ka turvaosaklasside tasemete tagamise mõttekust – näiteks S3 tagamise majanduslik otstarbekus.